Window Blinds

Employees can help lower energy costs and stabilize office temperatures by lowering window blinds when the outside temperature exceeds 70 degrees and direct sunlight is coming through the windows.

Electrical Appliances

No electrical appliances, other than coffee pots, may be used except in general use areas (e.g. lunchrooms).

Only coffee pots that have an automatic shut-off feature may be used within the office. Coffee pots must be plugged into a fixed receptacle (not an extension cord or furniture panel) and placed over a durable, stable surface, such as table on tile or carpet protectors.

Smoking

Smoking is allowed only in designated areas (see the door and gate access diagram for designated areas). Employees *may* smoke outside of door 8 and *may not* smoke outside of doors 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, and 13.

FredMeyer

6.2 Employee Entrance and Exit

(3/02)

Statement

All store, distribution center, retail service center, and plant employees must enter and exit through an employee door that has been designated.

Fred Meyer management reserves the right to inspect employee parcels, including the following:

- Packages or sacks
- Backpacks
- Lunch pails
- Briefcases
- Purses
- Empty boxes
- Any other container which could conceal merchandise

Employees who exit from a door other than the designated employee door(s) or who do not allow their parcels to be inspected are subject to disciplinary action up to and including termination.

Scope

This policy applies to store, distribution center, retail service center, and plant Fred Meyer Stores employees.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to the Vice President, Director of Loss Prevention.

Violation of this policy

Employees who violate this policy will be subject to disciplinary action up to and including termination.

FredMeyer

7 Systems and Communications

FredMeyer

7.1 Information Security

(7/99)

Statement

Information is valuable and a critical asset to Fred Meyer and the Company owns all rights to the information created or used on behalf of the Company. Measures are taken to protect it against unauthorized modification, disclosure, or destruction. Information is protected according to its value and sensitivity as well as to ensure its integrity, security, reliability, and availability.

Managing a profitable store requires the continuous flow of accurate information to forecast, project and alter decisions of the business. To ensure the accuracy of the information, protection must be exercised as to its integrity, security, reliability and availability. The identity of the authorized users must be verifiable.

Fred Meyer recognizes that the Company must comply with federal laws that apply to how certain information is disclosed, stored, retained, and destroyed. The policies and guidelines presented here are intended to help ensure the security and integrity of the Company's information and assets.

Definitions

The term *information* refers to data that is printed, written, or electronically stored and accessed in any phase of its life cycle, including its origination, processing, dissemination, and destruction.

Scope

This policy applies to all Fred Meyer Stores employees who have access to corporate information and assets, including all employees, contractors, vendors, and consultants.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to the Chief Information Officer.

Violation of this policy

Employees who violate this policy will be subject to disciplinary action up to and including termination.

Responsibilities

The following outlines the responsibilities of Information Services (IS), management personnel, and computer users:

Who	Responsible for—
Information Services (IS) Security Administration	IS Security Administration establish and implement policy regarding information security. They establish the standards, procedures, and guidelines necessary to ensure the security and integrity of information assets. They consult and review all matters affecting information security and provide support and policy enforcement tools to managers—assisting them in fulfilling their responsibilities.
Management Personnel	Managers and supervisors are responsible for the following: ✦ Ensuring the information within their assigned area of control is appropriately secured. This can be accomplished by working with Internal Audit and IS Security Administration to review, design, and implement controls ✦ Determining how information is disseminated, accessed, modified, retained, and disposed ✦ Informing their personnel that they are responsible for protecting the information they develop or use in the course of their jobs ✦ Identifying sensitive information that may require special handling inside or outside the department ✦ Ensuring personnel do not share user IDs or passwords ✦ Obtaining advance authorization from the Chief Information Officer, Group Vice President of Human Resources, or the Vice President, Director of Loss Prevention, before proceeding to investigate any communication media files

Continued on the next page...

Who	Responsible for—
Computer Users	All computer users are responsible for the following: ✦ All activity attributed to their user IDs ✦ Ensuring that the combination of their user IDs and passwords are not available for anyone else to use ✦ Understanding that all communications (both internal and external) transmitted or received within the Company are subject to inspection at any time, with or without notice—this includes electronic mail, voice mail, file cabinets, lockers, desks, postal mail addressed to Fred Meyer or mailed out from Fred Meyer premises, and faxes ✦ Ensuring that they do not use information tools for personal or nonbusiness reasons without prior approval from a supervisor

Responsibilities

The following outlines the responsibilities of store management and personnel:

Who	Responsible for—
Store Director	Store directors are responsible for implementing password and information security at the store level. They establish the standards, procedures, and guidelines necessary to ensure the security and integrity of information assets. They consult and review all matters affecting information security and provide support and policy enforcement tools to managers--assisting them in fulfilling their responsibilities

Continued on the next page...

Who	Responsible for—
Store Management	Managers and supervisors are responsible for the following: ✦ Ensuring the information within their assigned area of control is properly issued and secured ✦ Informing their personnel that they are responsible for protecting the information they use in the course of their jobs ✦ Ensuring personnel do not share passwords or user IDs ✦ Changing of password and authorization access in a timely manner as personnel changes ✦ Informing and identifying all systems where subordinates have authorized passwords ✦ Obtaining advance authorization from the Chief Information Officer, Group Vice President of Human Resources, or the Vice President, Director of Loss Prevention before proceeding to investigate any communication media files
Store Personnel	All employees are responsible for the following: ✦ All activity attributed to their user IDs ✦ Ensuring that the combination of their user IDs and passwords are not available for anyone else to use (for example: cash register systems, HRIS, OfficeVision, layaway or store alarm passwords) ✦ Understanding that all communications (both internal and external) transmitted or received within the Company are subject to inspection at any time, with or without notice—this includes electronic mail, voice mail, file cabinets, lockers, desks, postal mail addressed to Fred Meyer or mailed out from Fred Meyer premises, and faxes

Safeguarding user IDs and passwords

Fred Meyer computer systems require the entry of a valid user ID and/or password in order to gain access to certain applications (for example, electronic mail, merchandising, cash registers and store systems).

Users requiring access to an application must be individually authorized by their manager or supervisor. The sharing of user IDs or disclosure of passwords is a serious breach of Company policy and is grounds for disciplinary action up to and including termination.

Choosing a password

Passwords are intended to keep user IDs secure from use by others. Choosing a good password and changing it regularly is vital to ensuring that user IDs are kept private and not used by others. The computer system requires that computer users change their passwords periodically. Computer users should follow the guidelines below when choosing a password:

Do use...	Don't use...
Passwords between 6 and 8 characters in length	User IDs, birthdays, or dates
Two 3 or 4 letter words which are not related but easily remembered (like WISHFISH or DOGLOG)	Names, nicknames, or initials
The first or last letter of each word in a phrase (like NITTFAGM for "now is the time for all good men")	Slang, dictionary words, or common acronyms
A mixture of letters and numbers	Incrementing numbers (like JOHN01 or JOHN02) or repeating patterns (like JOHNxx or xxJOHN)

Logging on and off the system

Computer users should take the time to log on to the system correctly. Repeatedly entering the wrong password will *revoke* a computer user's user ID. If this occurs, the computer user should call the IS Help Desk to have his or her password reset.

To ensure information is kept secure, computer users should log off and lock their systems when leaving their work areas.

Distribution or disposal of printed information

Information safeguarded while it resides on a computer loses its safeguards when printed. Reports containing sensitive or confidential information left on tables, desks, in unlocked drawers, or tossed in the recycle bin can expose information to unintended disclosure or theft.

When distributing a sensitive report, place the report in a sealed envelope marked CONFIDENTIAL; then put it into another envelope (such as an intersection mail envelope) that does not indicate the confidential nature of the enclosed material.

Questions

Any computer user with questions about security or information responsibilities should contact IS Security Administration.

Any store employee with questions about passwords should contact his or her department manager or store director.

Any computer user with questions about passwords should contact the IS Help Desk.

Related policies

For specific guidelines relating to electronic mail, refer to corporate policy *7.5 Electronic Mail.*

FredMeyer

7.2 Software Copyright Laws

(12/91)

Statement

It is Fred Meyer policy to comply with all federal microcomputer copyright laws. Possession and/or use of licensed microcomputer software at Fred Meyer will be strictly enforced.

All Fred Meyer employees are responsible for using the software purchased for their microcomputers in accordance with the guidelines stated in this policy. Fred Meyer will enforce a strict policy on software use to avoid exposure to serious legal liability.

Software audits will be made periodically by internal and/or external auditors to ensure compliance.

Scope

This policy applies to all Fred Meyer Stores employees and will be enforced by all levels of management.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to the Network Services Manager.

Violation of this policy

Employees who violate this policy will be subject to disciplinary action up to and including termination.

Stand-alone microcomputers

Each microcomputer software program that the Company licenses can be used on only one microcomputer at a time. If a microcomputer has software loaded on its hard disk then that particular software should not be loaded onto any other hard disk. For example, if a department has 10 microcomputers with Lotus 1-2-3 installed on each one, then that department must have 10 valid sets of Lotus 1-2-3 programs registered on the corporate database. All original system disks or license agreements (proof of purchase) are maintained on file in the software library.

Microcomputers linked to local area networks

Most departments within the Company are hooked up to local area networks (LANs), which make use of special site-licensing agreements or LAN versions of software. This allows the Company to provide simultaneous access to more than just one user.

Software may not be copied from the file server onto individual microcomputer hard disks. Additionally, software licensed to an individual workstation may not be copied to the file server.

Duplicating software

Network Services makes one backup copy of each software program for archival purposes. It is illegal to make copies of software for any other purposes.

Employees must not make unauthorized copies of software or any accompanying documentation, including software installed on a LAN for network use. Any employee found copying software for reasons other than for backup or archival purposes will be subject to legal fines and/or disciplinary action up to and including termination.

Using company software at home

Software purchased by Fred Meyer may not be used on personally owned microcomputers. System disks and backup copies must remain on Fred Meyer premises at all times.

Giving software to outside third parties

Microcomputer software is a corporate asset. Employees found giving software to outside third parties (including relatives, friends, clients, or Customers) are subject to disciplinary action up to and including termination.

FredMeyer

7.3 Purchasing Microcomputer Hardware/ Software

(5/96)

Statement

This policy provides Fred Meyer with the means to manage microcomputer hardware and software purchases throughout the Company. This type of management is necessary to:

- Help users select the right equipment and tools for the job
- Support the various software packages and hardware platforms
- Obtain appropriate budgetary authorization
- Maintain a current asset list of Company hardware and software

Scope

This policy applies to all Fred Meyer Stores employees.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to the Network Services Manager.

Violation of this policy

Employees who violate this policy will be subject to disciplinary action up to and including termination.

Process overview

The following explains the process for requesting all hardware and software purchases. It is mandatory that all purchases of this type be approved by Information Services (IS).

Determine the need for the microcomputer hardware and/or software. ***If it is needed as part of an IS project,*** the request becomes part of the overall project—software and hardware costs become part of the system justification. *If it is needed for a stand-alone microcomputer,* follow the process below:

Stage	What Happens
1	Requestor (user) completes a *Project/Fixture Request* form (M1234) and obtains the signature of an assistant vice president or above.
2	Requestor submits request to Network Services.
3	Network Services project manager is assigned to review the request, make recommendation(s), and provide cost estimate(s).
4	Requestor and Network Services project manager select the best option and obtain approval from Network Services management team.
5	**If the request is approved,** Network Services purchases and installs hardware and/or software. **If the request is denied,** the requestor and Network Services project manager either try another option or further explain the business need and/or benefit of the request.

Guidelines for purchasing/leasing hardware or software

All microcomputer hardware and software purchases must be placed by Network Services.

Any hardware or software leases must be initiated by Network Services. Generally, leasing is not considered the most cost-effective solution.

Software installation and original disks

Anytime new software is purchased, Network Services installs it on the appropriate microcomputer. A backup copy of the software is then made for the user, and the original disk(s) are kept in a central software library. Do not attempt to install, remove, or copy (except for backup purposes) software from microcomputers without assistance from Network Services.